DOI: 10.19783/j.cnki.pspc.181345

基于非线性状态估计的虚假数据注入攻击代价分析

赵丽莉[1,2]，刘忠喜[3]，孙国强[3]，倪 明[1,2]

(1. 南瑞集团有限公司，江苏 南京 211106；2. 国电南瑞科技股份有限公司，江苏 南京 211106；
3. 河海大学，江苏 南京 211100)

摘要：随着智能电网的发展，信息通信系统与物理电力系统深度融合，虚假数据注入等网络攻击可能会对电网的安全稳定造成严重影响，目前这方面研究已成热点问题。一次成功的虚假数据注入攻击涉及攻击者所掌握资源、攻击区域选择和攻击向量构建。在有限的资源下，根据实际电网运行特征，以攻击节点为中心，构建了单节点攻击区域和多节点攻击区域，一定程度上可缩小攻击范围。基于非线性状态估计模型，分别针对单节点攻击与多节点攻击情形，提出一种掌握局部电网信息下的攻击代价分析方法。最后以 IEEE-14 系统和 IEEE-1354 系统为例，分别进行单节点攻击和多节点攻击分析，其结果验证了所提虚假数据注入攻击代价分析方法的有效性。

关键词：虚假数据注入；攻击代价；信息安全；信息物理系统；非线性；多节点攻击

Cost analysis of the false data injection attack based on nonlinear state estimation

ZHAO Lili[1,2], LIU Zhongxi[3], SUN Guoqiang[3], NI Ming[1,2]

(1. NARI Group Co., Ltd., Nanjing 211106, China; 2. NARI Technology Co., Ltd., Nanjing 211106, China;
3. Hohai University, Nanjing 211100, China)

Abstract: With the development of smart grid, physical power system has been coupled with cyber and communication system deeper and deeper. Attacks against the cyber and communication system such as False Data Injection (FDI) may cause fatal influences on the security and stability of power system, researches about it has become hot topics at present. One successful FDI attack has to take resources owed by an attacker, the selection of attack area and the building of attack vector into consideration. With limited resources, the single-node and the multi-node attack areas are built around the attacked nodes according to the operation characteristics of the real power system, which can narrow the scale of an attack in some degree. Based on the nonlinear state estimation model, an attack cost analysis method is proposed with limited power system information for the single-node and the multi-node attacks. Lastly, IEEE-14 and IEEE-1354 power systems are applied for the effectiveness of the FDI attack cost analysis proposed by the paper in the situations of the single-node and the multi-node attacks.

This work is supported by Science and Technology Project of State Grid Corporation of China “Identification Method of Malicious Attack on the Power Grid and Active Defense Method on the Power Grid Side” (No. 524608170138) and Project of Jiangsu Economic and Information Technology Commission “Research of Key Technologies and Platform Development of Cyber Physical Power System Co-Simulation” (No. 524608170191).

Key words: false data injection; attack cost; cyber security; cyber-physical system; non-linear; multi-node attack

0 引言

随着智能电网的发展，电网已然是由信息通信系统和物理电力系统深度耦合的系统[1-2]。信息通信技术的渗透一方面提升了电网运行的信息化和智能化，另一方面带来了信息系统安全的隐患，可能会使智能电网的安全经济运行遭受威胁[3-5]。近 20 年来，电网多次因信息通信网络被攻击而发生重大事故，如 2000 年 10 月中国二滩电厂因接收到异常信号停机险致川渝电网崩溃瓦解，2015 年 12 月网络攻击致使乌克兰电网发生大规模停电事故[6]。

基金项目：国家电网公司科技项目“电网恶意攻击的辨识方法及电网侧主动防御方法研究”资助(524608170138)；江苏经信委项目“信息物理电力系统综合仿真关键技术研究和平台开发”资助(524608170191)

虚假数据注入攻击的概念于 2009 年第一次被提出[7]，即通过有组织、有预谋地破解量测设备的密码系统进行数据篡改或者通过光纤窃听技术截获并篡改数据采集与监视控制(Supervisory Control And Data Acquisition, SCADA)系统传送至控制中心的数据，达到干扰状态估计结果的目的。目前，虚假数据注入攻击已是热点问题，相关研究成果颇多，主要集中在攻击策略、攻击影响及应对攻击的安全防御措施 3 个方面[8]。

就攻击策略而言，众学者站在攻击者的角度，揣测攻击者的心态和处境，提出了很多方法。早期的攻击构建主要基于直流模型，易被实际电力系统中基于交流模型的坏数据辨识环节发现，成功率较低。因此相关研究展开对基于交流模型的攻击构建方法的探索，并取得一定成果。上述研究根据攻击者掌握信息的程度即对电网拓扑和参数信息的掌握程度分为掌握电网全局信息[9-10]和局部信息[11-12]两种情况。相对来说，掌握电网全局信息下的攻击成功率较高一些，但局部信息掌握情况下的攻击更符合实际。攻击者获取的电网拓扑和参数信息一般精度稍差，文献[13]给出了此种情形下的攻击构建方法。从攻击者的角度来说，会想尽办法以最少的攻击成本即攻击最少的量测达到高效的攻击。目前研究主要从攻击向量的稀疏性着手来优化攻击[14-16]，并提出多种求解方法，如启发式算法和贪婪搜索算法。

在攻击者掌握有限资源的情况下，本文考虑电网单个节点和多个节点上的量测设备遭受攻击这两种情形，构建攻击区域，提出一种攻击代价的量化分析方法。以 IEEE-14 系统和 IEEE1354 系统为例，分别针对单节点攻击和多节点攻击两种情形进行分析，验证所提攻击代价量化分析法的有效性，希望为网络攻击防范提供参考。

1　虚假数据注入攻击原理

在电力系统状态估计中，量测数据类型包括：节点注入有功和无功功率、支路有功和无功功率、节点电压幅值，它们与节点电压幅值和相角等状态量之间满足如式(1)的关系[17]。

$$\boldsymbol{z}=\boldsymbol{h}(\boldsymbol{x})+\boldsymbol{e} \tag{1}$$

式中：$\boldsymbol{z}=[z_1,z_2,\cdots,z_m]^{\mathrm{T}}$ 表示 m 维量测矢量；$\boldsymbol{x}=[x_1, x_2,\cdots,x_{2n-1}]^{\mathrm{T}}$ 表示 $2n-1$ 维状态矢量；n 为电力系统节点数；$\boldsymbol{h}(\bullet)$表示交流电网模型下的状态估计非线性函数；$\boldsymbol{e}=[e_1,e_2,\cdots,e_m]^{\mathrm{T}}$ 为 m 维量测噪声矢量，主要来源于量测设备的量测误差和传输过程中信号干扰造成的误差。

由于量测噪声的存在，量测数据中会有少量的坏数据，这会降低状态估计的精度，坏数据较多时甚至有可能造成状态估计的不收敛。因此，实际中还会在状态估计的基础上增加坏数据的辨识环节，常采用的坏数据辨识方法主要基于残差进行检测。其中，残差可表示为

$$\boldsymbol{r}=\left\|\boldsymbol{z}-\boldsymbol{h}(\tilde{\boldsymbol{x}})\right\|_2 \tag{2}$$

式中：$\tilde{\boldsymbol{x}}$ 为系统状态量估计值；$\boldsymbol{r}$ 为残差，当残差大于检测门槛值 τ 时说明量测中存在坏数据。

若要保证攻击成功，则需使得基于非线性状态估计构建的攻击向量能躲过坏数据的辨识。理想情况下，攻击者发起虚假数据注入攻击，向原量测矢量中输入攻击向量 $\boldsymbol{a}$，得到新的量测矢量 $\boldsymbol{z}_{\mathrm{a}}=\boldsymbol{z}+\boldsymbol{a}$，状态估计程序接收到的量测矢量实际为攻击后的 $\boldsymbol{z}_{\mathrm{a}}$，此时的量测已较实际量测发生偏差，由此得到的状态估计值亦将发生偏差，经虚假数据注入攻击后，残差为

$$\boldsymbol{r}_{\mathrm{a}}=\boldsymbol{z}_{\mathrm{a}}-\boldsymbol{h}(\tilde{\boldsymbol{x}}_{\mathrm{bad}}) \tag{3}$$

式中：$\tilde{\boldsymbol{x}}_{\mathrm{bad}}=\tilde{\boldsymbol{x}}+\boldsymbol{c}$，表示虚假数据注入攻击后的系统状态量估计值；$\boldsymbol{r}_{\mathrm{a}}$ 表示虚假数据注入攻击后的残差。

攻击后只要保证残差小于等于坏数据检测门槛值 τ，虚假数据注入攻击便可躲过坏数据辨识环节，达到成功篡改状态估计结果的目的。

2　攻击区域构建

在现有研究中将假数据注入攻击分成三种模式：随机注入攻击、有目标无约束攻击和有目标有约束攻击[7,13]。随机注入攻击即攻击随意量测数据且攻击数量不限，同时不考虑攻击是否成功及攻击后状态估计结果的变化。有目标无约束攻击则是攻击特定数量的状态量，同时保证本次攻击不被坏数据辨识模块发现；有目标有约束的攻击则是在上一种攻击场景条件下，攻击尽可能少的量测数据。

为保证攻击成功率，通常会对特殊节点(包括发电机节点和零注入节点)进行特殊处理。基本原则如下：1) 不会篡改发电机的有功和无功量测，因为发电厂控制室与电力系统控制中心直接通信，量测量的突变等异常易被检测出，导致虚假数据注入攻击失败；2) 对零注入节点，在篡改与之相关联支路的有功和无功量测时，要确保篡改后依然是零注入节点。另外需要注意的是负荷量测的篡改幅度，一般为负荷实际值的 50%~150%[7]。

基于上述原则，假定攻击者只能篡改至多 k 个电力节点的状态估计值，构建有目标有约束攻击集

合 $\Gamma=\{i_1,i_2,\cdots,i_k\}$，该集合由被攻击的电力节点组成，集合中元素为节点编号。

攻击区域的选择在一定程度上决定了攻击代价的大小，有赖于攻击者对电网拓扑和结构参数的掌握程度及攻击目标的选定。实际中，由于电网规模的庞大及动态运行，攻击者很难完全准确地掌握电网的全部信息，只能获得局部区域信息，另一方面考虑攻击代价，将会对局部区域进行相关量测的篡改。本文借鉴文献[13]的最优攻击区域确定的思想进行攻击区域的构建。攻击区域形成流程如图 1 所示，具体步骤如下。

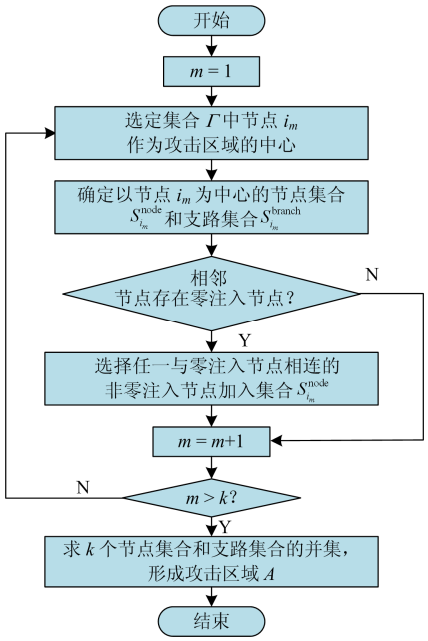

图 1 攻击区域形成流程图

Fig. 1 Flow chart of the attack area building

1) 令 $m=1$；

2) 选定集合 Γ 中某个电力节点 i_m 作为攻击区域的中心；

3) 确定以节点 i_m 为中心的区域内的节点集合 $S_{i_m}^{node}$(此处，$S_{i_m}^{node}$ 包括节点 i_m 及与之连接的节点)和支路集合 $S_{i_m}^{branch}$；

4) 查看与节点 i_m 连接的节点中是否存在零注入节点，若存在，形成零注入节点集合 P，转入步骤 5)，若不存在转入步骤 6)；

5) 针对集合 P 中的每一个零注入节点，选择任意一个与之连接的非零注入节点，加入集合 $S_{i_m}^{node}$ 中；

6) 此时节点集合 $S_{i_m}^{node}$ 已完整，集合 $S_{i_m}^{branch}$ 包括集合 $S_{i_m}^{node}$ 中与节点 i_m 相连的所有支路和零注入节点与其他节点间的连接支路，$m=m+1$，若 $m\le k$ 返回步骤 2)，若 $m>k$ 转入步骤 7)；

7) 最终的攻击区域 A 确定如下：

设以每个被攻节点 i_m 为中心形成的单节点攻击区域为 A_{i_m}，则

$$A_{i_m}=S_{i_m}^{node}\cup S_{i_m}^{branch} \tag{4}$$

设多节点攻击区域为 A，则

$$A=\bigcup_{m=1}^{k}A_{i_m} \tag{5}$$

攻击区域 A 中的节点集合 S^{node} 为

$$S^{node}=\bigcup_{m=1}^{k}S_{i_m}^{node} \tag{6}$$

攻击区域 A 中的支路集合 S^{branch} 为

$$S^{branch}=\bigcup_{m=1}^{k}S_{i_m}^{branch} \tag{7}$$

3　攻击代价分析

早期的虚假数据注入攻击研究主要基于直流系统线性状态估计模型[7, 18-20]，因其对实际交流电网的近似而使得构建的虚假数据注入攻击与预期的存在一定偏差。因此，一些研究考虑实际电网的非线性特征，尝试基于交流系统状态估计模型(如最小二乘法、快速分解法等)构建虚假数据注入攻击[21-23]。本文基于交流潮流模型构建掌握局部信息时的攻击。

由极坐标系下的电力系统网络方程可知，节点注入有功功率和无功功率可以表示为

$$P_i=\sum_{j\in N_i}V_iV_j\left[G_{ij}\cos(\theta_i-\theta_j)+B_{ij}\sin(\theta_i-\theta_j)\right] \tag{8}$$

$$Q_i=\sum_{j\in N_i}V_iV_j\left[G_{ij}\sin(\theta_i-\theta_j)-B_{ij}\cos(\theta_i-\theta_j)\right] \tag{9}$$

式中：P_i、Q_i 分别为节点 i 的注入有功功率、无功功率；V_i、V_j 分别为节点 i、j 的电压幅值；θ_i、θ_j 分别为节点 i、j 的电压相角；G_{ij}、B_{ij} 分别为节点 i 与电力节点 j 之间支路电导、电纳；N_i 为节点 i 及与其相连的电力节点构成的集合。

支路有功功率和无功功率可以表示为

$$p_{ij}=V_i^2g-V_iV_j\left[G_{ij}\cos(\theta_i-\theta_j)+B_{ij}\sin((\theta_i-\theta_j)\right] \tag{10}$$

$$q_{ij}=-V_i^2b-V_iV_j\left[G_{ij}\sin(\theta_i-\theta_j)-B_{ij}\,cos\,(\theta_i-\theta_j)\right] \tag{11}$$

式中：p_{ij}、q_{ij} 分别为节点 i 与节点 j 之间支路有功功率、无功功率；g 为支路对地电导；b 为支路对地导纳。

由式(8)—式(11)可以看出，节点 i 的注入功率及与节点相连的支路潮流均会因节点 i 的状态量的改变而发生偏差。为保证虚假数据注入攻击躲过坏

数据辨识模块，攻击者需根据电力系统网络方程构建虚假数据注入攻击向量，保证其一致性。据此，式(3)可进一步写为

$$\begin{aligned}&\boldsymbol{r}_{\mathrm{a}}=\boldsymbol{z}_{\mathrm{a}}-\boldsymbol{h}(\tilde{\boldsymbol{x}}_{\mathrm{bad}})=\\&\quad\boldsymbol{z}-\boldsymbol{h}(\tilde{\boldsymbol{x}})+\boldsymbol{a}-\left[\boldsymbol{h}(\tilde{\boldsymbol{x}}_{\mathrm{bad}})-\boldsymbol{h}(\tilde{\boldsymbol{x}})\right]=\\&\quad\boldsymbol{r}+\boldsymbol{a}-\left[\boldsymbol{h}(\tilde{\boldsymbol{x}}_{\mathrm{bad}})-\boldsymbol{h}(\tilde{\boldsymbol{x}})\right]\end{aligned}\tag{12}$$

此时，攻击向量的约束方程为

$$\boldsymbol{a}=\left[\boldsymbol{h}(\tilde{\boldsymbol{x}}_{\mathrm{bad}})-\boldsymbol{h}(\tilde{\boldsymbol{x}})\right]+\boldsymbol{r}_{\mathrm{a}}-\boldsymbol{r}\tag{13}$$

为使攻击前后电力系统状态“未发生改变”(实际已被篡改)，通常会使攻击前后残差保持一致，即 $\boldsymbol{r}_{\mathrm{a}}=\boldsymbol{r}$，那么攻击向量 $\boldsymbol{a}$ 可由式(14)求得

$$\boldsymbol{a}=\boldsymbol{h}(\tilde{\boldsymbol{x}}_{\mathrm{bad}})-\boldsymbol{h}(\tilde{\boldsymbol{x}})\tag{14}$$

假设攻击者所能攻击的电力节点个数不超过 k 个，根据第 2 节中原则篡改功率量测，以间接篡改目标电压相角状态量到特定值。设攻击向量 $\boldsymbol{a}$ 中非零元素个数为 M_a，则虚假数据注入攻击代价可表示为

$$\begin{aligned}&M_{\mathrm{a}}=\left\|\boldsymbol{h}(\tilde{\boldsymbol{x}}_{\mathrm{bad}})-\boldsymbol{h}(\tilde{\boldsymbol{x}})\right\|_0\\&\text{s.t.}\quad\left\|\tilde{\boldsymbol{x}}_{\mathrm{bad}}-\tilde{\boldsymbol{x}}\right\|=k\end{aligned}\tag{15}$$

3.1 单节点攻击

假定攻击者希望篡改节点 i 的电压相角 θ_i 到指定值，此时

$$\theta_i'-\theta_j=\theta_i+c_i-\theta_j\tag{16}$$

式中，c_i 为节点 i 的电压相角 θ_i 在遭受虚假数据注入攻击后的偏差。

以节点 i 为中心，按照第 2 节的方法形成攻击区域 A_i，其对应的节点集合 S_i^{node} 和支路集合 S_i^{branch} 的元素个数计算为

$$N_i=card\left(S_i^{\mathrm{node}}\right)\tag{17}$$

$$B_i=card\left(S_i^{\mathrm{branch}}\right)\tag{18}$$

在全量测系统中，攻击者需篡改攻击区域 A_i 中每个节点的注入有功和无功功率量测值(发电机节点和零注入节点除外)以及支路的有功和无功功率量测值。针对非全量测系统，攻击者完成攻击所需要修改的量测数据个数会有所减少。令 υ_n 为每个节点注入功率量测个数，ω_b 为支路功率量测个数，设区域 A_i 中发电机节点个数为 γ_i(若发电机节点为非量测点，则认为 $\gamma_i=0$)，零注入节点个数为 η_i(若零注入节点为非量测点，则认为 $\eta_i=0$)，则攻击代价即需篡改的量测数据个数为

$$H_i=\sum_{n=1}^{N_i}\upsilon_n+\sum_{b=1}^{B_i}\omega_b-2\left(\gamma_i+\eta_i\right)\tag{19}$$

3.2 多节点攻击

当对 k 个节点攻击时，假定攻击节点集合为 $\Gamma=\{i_1, i_2, \cdots, i_k\}$，由第 2 节中方法可形成攻击区域 A，其对应的节点集合为 S^{node} 和 S^{branch}，集合元素个数为

$$N=card\left(S^{\mathrm{node}}\right)\tag{20}$$

$$B=card\left(S^{\mathrm{branch}}\right)\tag{21}$$

则多节点攻击时攻击代价计算公式与单节点攻击时一致，即多节点攻击时攻击代价为

$$H=\sum_{n=1}^{N}\upsilon_n+\sum_{b=1}^{B}\omega_b-2\left(\gamma+\eta\right)\tag{22}$$

式中：γ、η 分别为攻击区域 A 中发电机节点个数(若发电机节点为非量测点，则认为 $\gamma=0$)和零注入节点个数(若零注入节点为非量测点，则认为 $\eta=0$)。

若攻击节点集合 Γ 中存在具有相连支路的两个节点 i 和 j，且篡改后电压相角偏差相同，即 $c_i=c_j$，那么攻击区域 A 中节点 i 和节点 j 之间支路上的有功功率 $\tilde{p}_{ij}$、$\tilde{p}_{ji}$ 和无功功率 $\tilde{q}_{ij}$、$\tilde{q}_{ji}$ 量测在攻击前后不发生改变，因为

$$\theta_i'-\theta_j'=\theta_i-\theta_j+c_i-c_j\tag{23}$$

式中：c_j 为节点 j 的电压相角 θ_j 在遭受虚假数据注入攻击后的偏差。

将式(23)代入式(10)和式(11)可知攻击前后支路有功功率 p_{ij}、p_{ji} 和无功功率 q_{ij}、q_{ji} 不会发生改变。则式(22)重新写为

$$H=H^{\mathrm{node}}+H^{\mathrm{branch}}-2(\gamma+\eta)\tag{24}$$

式中，H_N 和 H_B 分别为节点量测总数和支路量测总数，具体为

$$H^{\mathrm{node}}=\sum_{n=1}^{N}\upsilon_n,\quad H^{\mathrm{branch}}=\sum_{b=1}^{B}\zeta_b$$

$$\zeta_b=\begin{cases}\omega_b & c_i\neq c_j\\0 & c_i=c_j\end{cases},$$

此处，$c_i=c_j$ 表示支路 b 两端节点电压相角偏差相等；$c_i\neq c_j$ 表示支路 b 两端节点电压相角偏差不相等。

4　算例分析

4.1 针对 IEEE-14 系统的攻击分析

以 IEEE-14 节点系统(如图 2 所示)为例，为全量测系统，其量测数据包括节点注入有功功率量测 12 个，节点注入无功功率量测 13 个，支路有功功率量测 40 个，支路无功功率量测 40 个，节点电压量测 14 个，共计 119 个。选择 MATPOWER 中潮流计算值作为真值，并在真值的基础上叠加高斯噪

声得到量测值，其中量测数据标准差 $\sigma_e = 0.01$，部分数值如表 1 所示。

表 1 IEEE-14 节点电力系统量测数据

Table 1 Measurements of the IEEE-14 power system

量测位置	量测数据	真值	量测值
节点 6	P_6	−0.112	−0.125
	Q_6	0.052	0.067
节点 9	P_9	−0.295	−0.299
	Q_9	−0.166	−0.152
节点 12	P_{12}	−0.061	−0.033
	Q_{12}	−0.016	−0.009
节点 13	P_{13}	−0.135	−0.148
	Q_{13}	−0.058	−0.042
节点 14	P_{14}	−0.149	−0.119
	Q_{14}	−0.050	−0.045
支路 6-12	$P_{6\text{-}12}$	0.078	0.078
	$Q_{6\text{-}12}$	0.025	0.028
	$P_{12\text{-}6}$	−0.077	−0.074
	$Q_{12\text{-}6}$	−0.024	−0.022
支路 6-13	$P_{6\text{-}13}$	0.177	0.181
	$Q_{6\text{-}13}$	0.072	0.088
	$P_{13\text{-}6}$	−0.175	−0.184
	$Q_{13\text{-}6}$	−0.068	−0.076
支路 9-14	$P_{9\text{-}14}$	0.094	0.095
	$Q_{9\text{-}14}$	0.036	0.037
	$P_{14\text{-}9}$	−0.093	−0.105
	$Q_{14\text{-}9}$	−0.034	−0.026
支路 12-13	$P_{12\text{-}13}$	0.016	0.031
	$Q_{12\text{-}13}$	0.008	0.009
	$P_{13\text{-}12}$	−0.016	−0.024
	$Q_{13\text{-}12}$	−0.007	−0.008
支路 13-14	$P_{13\text{-}14}$	0.056	0.060
	$Q_{13\text{-}14}$	0.017	−0.002
	$P_{14\text{-}13}$	−0.056	−0.058
	$Q_{14\text{-}13}$	−0.016	−0.021

1) 单节点攻击

以 13 号节点为攻击目标，与之相连的支路为 6-13、12-13 和 13-14，即 $S_{13}^{\text{node}} = \{6,12,13,14\}$，$S_{13}^{\text{branch}} = \{6\text{-}13,12\text{-}13,13\text{-}14\}$。

节点集合中无零注入节点，6 号节点上虽然有发电机，但因为同时还有负荷，所以可以篡改 6 号节点的量测，此处认为发电机节点个数为 0。由式(17)—式(19)可求得单节点攻击时攻击代价即需篡改的量测数为 20 个。

假定攻击后 13 号节点的电压相角偏差 $c_{13} = -1.5°$，基于式(14)可求得攻击向量，其非零元素值如表 2 所示。攻击向量的非零元素共 20 个，与单节点攻击代价分析计算所得需篡改量测数一致。将攻击向量叠加到量测数据上，并进行状态估计计算。此时 θ_{13} 由原来的−15.2°降低为−16.75°，$\Delta\theta_{13} = -1.55° \approx c_{13}$，同时系统的残差由 0.084 降低为 0.077，在坏数据辨识的阈值范围内。结合表 1 和表 2 可知，攻击区域内的三条支路 6-13、12-13 和 13-14 其攻击后的支路潮流量测值相比攻击前增长至少 1 倍，尤其是支路 12-13 攻击后的潮流量测值是攻击前的 5 倍多，这个值极有可能已超过其传输功率极限，将诱骗控制中心作出错误判断，认为线路过载而采取相关保护措施(如切负荷等)，可能引发电网发生安全稳定事故，造成重大经济损失。

表 2 IEEE-14 系统中单节点攻击向量非零元素值

Table 2 Non-zero elements of single-node attack vector of the IEEE-14 system

ΔP_i	ΔQ_i	$\Delta p_{i\text{-}j}$	$\Delta q_{i\text{-}j}$
ΔP_6=0.19	ΔQ_6=−0.09	$\Delta p_{6\text{-}13}$=0.20	$\Delta q_{6\text{-}13}$=−0.09
ΔP_{12}=0.09	ΔQ_{12}=−0.07	$\Delta p_{13\text{-}6}$=−0.18	$\Delta q_{13\text{-}6}$=0.10
		$\Delta p_{12\text{-}13}$=0.07	$\Delta q_{12\text{-}13}$=−0.07
ΔP_{13}=−0.31	ΔQ_{13}=0.21	$\Delta p_{13\text{-}12}$=−0.05	$\Delta q_{13\text{-}12}$=0.07
		$\Delta p_{13\text{-}14}$=−0.07	$\Delta q_{13\text{-}14}$=0.04
ΔP_{14}=0.06	ΔQ_{14}=−0.03	$\Delta p_{14\text{-}13}$=0.06	$\Delta q_{14\text{-}13}$=−0.04

2) 多节点攻击

以 12~14 号节点为攻击目标，与 12 号节点相连的支路为 6-12、12-13；与 13 号节点相连的支路为 6-13、12-13、13-14；与 14 号节点相连的支路为 9-14、13-14。则攻击区域 A(如图 2 中的红色标注)可由节点集合 $S^{\text{node}} = \{6,9,12,13,14\}$ 和支路集合 $S^{\text{branch}} = \{6\text{-}12,6\text{-}13,9\text{-}14,12\text{-}13,13\text{-}14\}$ 表示。

假定攻击后 12~14 号节点的电压相角偏差 $c_{12} = c_{13} = c_{14} = -1.5°$，由图 2 可知，12、13、14 号节点间有支路相连，且攻击区域 A 的节点集合中无发电机节点也无零注入节点，由式(20)、式(21)和式(24)可求得当对 12、13、14 号节点进行虚假数据注入攻击时需篡改的量测数为 22 个。若 12、13 和 14 号电压相角偏差不等，则需篡改的量测数为 30 个，也就是说攻击者需额外注入 8 个虚假数据，攻击代价增长约 36%。

基于式(14)求得攻击向量中非零元素(如表 3 所示)共 22 个，与多节点攻击代价分析计算所得需篡改量测数一致。将攻击向量叠加到量测数据上，再次进行状态估计计算。此时 θ_{12} 由原来的−14.9°降低为−16.5°，$\Delta\theta_{12} = -1.6° \approx c_{12}$；$\theta_{13}$ 由原来的−15.2°降低为−16.75°，$\Delta\theta_{13} = -1.55° \approx c_{13}$；$\theta_{14}$ 由原来的−16°降低为−17.55°，$\Delta\theta_{14} = -1.55° \approx c_{14}$。同时，系统的残差由 0.084 降低为 0.072，在坏数据辨识的阈值范围内。因为 c_{12}=c_{13}=c_{14}，由式(10)、式(11)和式(23)

可知此时支路 12-13，13-14 的有功和无功功率没有发生改变，不需要额外的虚假数据注入，所以当发起多节点攻击时，若攻击区域中被攻击节点间有支路相连且两端节点的电压相角篡改偏差相等，则可使攻击区域内需篡改的量测数减少。

表 3 IEEE-14 系统多节点攻击向量非零元素值

Table 3 Non-zero elements of multi-node attack vector of the IEEE-14 system

ΔP_i	ΔQ_i	$\Delta p_{i\text{-}j}$	$\Delta q_{i\text{-}j}$
ΔP_6=0.28	ΔQ_6=−0.13	$\Delta p_{6\text{-}12}$=0.09	$\Delta q_{6\text{-}12}$=−0.05
ΔP_9=0.84	ΔQ_9=−0.03	$\Delta p_{12\text{-}6}$=−0.11	$\Delta q_{12\text{-}6}$=0.04
ΔP_{12}=−0.07	ΔQ_{12}=0.05	$\Delta p_{6\text{-}13}$=0.20	$\Delta q_{6\text{-}13}$=−0.09
		$\Delta p_{13\text{-}6}$=−0.18	$\Delta q_{13\text{-}6}$=0.10
ΔP_{13}=−0.18	ΔQ_{13}=0.10	$\Delta p_{9\text{-}14}$=0.10	$\Delta q_{9\text{-}14}$=−0.04
ΔP_{14}=−0.10	ΔQ_{14}=0.06	$\Delta p_{14\text{-}9}$=−0.09	$\Delta q_{14\text{-}9}$=0.05

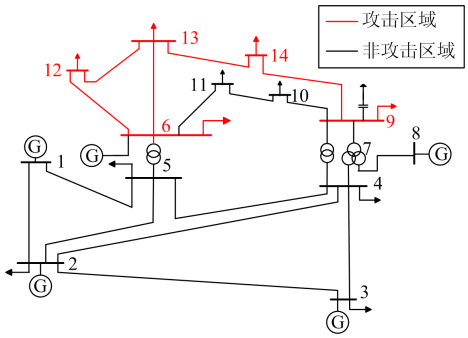

图 2 IEEE-14 节点电力系统

Fig. 2 IEEE-14 power system

另外结合表 1 和表 3 发现：由于节点 12、13 和 14 的电压相角偏差相同，所以攻击区域内支路 12-13 和 13-14 的潮流量测值攻击前后并未发生变化；其他支路潮流量测值与单节点攻击时类似，相比攻击前增长至少 1 倍，如果攻击前这些线路的负载率本就已很高，如达到 70%，那么攻击后控制中心人员所看到的将是这些线路已过载，需采取相关保护措施，这对电网的安全运行不利。

4.2 针对 IEEE-1354 系统的攻击分析

以 IEEE-1354 系统(全量测系统)为例，进一步验证本文所提攻击成本分析方法的有效性。与 4.1 节类似，分别对 IEEE-1354 系统进行单节点攻击和多节点攻击分析。攻击区域如图 3 所示，共 4 个零注入节点，0 个发电机节点。攻击分析涉及到的相关量测值如表 4 所示。

单节点攻击：以节点 34 为攻击目标，使其电压相角偏差−1.5°。其攻击区域由 S_{34}^{node} ={10,34,219, 893,1310,1349} 和 S_{34}^{branch} ={10-34,10-893,34-219, 1310-1349,893-1310} 组成。

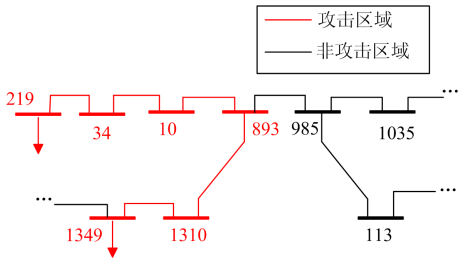

图 3 IEEE-1354 节点电力系统攻击区域

Fig. 3 Attack area of the IEEE-1354 power system

表 4 IEEE-1354 节点电力系统量测数据

Table 4 Measurements of the IEEE-1354 power system

量测位置	量测数据	真值	量测值
节点 219	P_{219}	−1.25	−1.29
	Q_{219}	−0.46	−0.36
节点 1349	P_{1349}	−6.41	−6.39
	Q_{1349}	0.57	0.58
节点 10	P_{10}	0	0
	Q_{10}	0	0
节点 34	P_{34}	0	0
	Q_{34}	0	0
节点 893	P_{893}	0	0
	Q_{893}	0	0
节点 1310	P_{1310}	0	0
	Q_{1310}	0	0
支路 34-219	$P_{34\text{-}219}$	1.25	1.26
	$Q_{34\text{-}219}$	0.52	−0.51
	$P_{219\text{-}34}$	−1.25	−1.28
	$Q_{219\text{-}34}$	−0.47	−0.51
支路 893-1310	$P_{893\text{-}1310}$	−2.51	−2.52
	$Q_{893\text{-}1310}$	−0.54	−0.55
	$P_{1310\text{-}893}$	2.52	2.53
	$Q_{1310\text{-}893}$	0.61	0.59
支路 1310-1349	$P_{1310\text{-}1349}$	−1.74	1.72
	$Q_{1310\text{-}1349}$	−0.53	−0.51
	$P_{1349\text{-}1310}$	1.74	1.74
	$Q_{1349\text{-}1310}$	0.55	0.54
支路 10-34	$P_{10\text{-}34}$	2.81	2.82
	$Q_{10\text{-}34}$	0.20	0.18
	$P_{34\text{-}10}$	−2.81	−2.81
	$Q_{34\text{-}10}$	−0.16	−0.15
支路 10-893	$P_{10\text{-}893}$	−2.59	−2.59
	$Q_{10\text{-}893}$	−0.18	−0.18
	$P_{893\text{-}10}$	2.59	2.59
	$Q_{893\text{-}10}$	0.23	0.23

多节点攻击：以节点 10、34、893 为攻击目标，使其电压相角偏差−1.5°。其攻击区域由 S^{node} ={10,34,219,893,1310,1349} 和 S^{branch} ={10-34,10-893,

34-219,1310-1349,893-1310}组成。

攻击后，重新进行状态估计计算，攻击目标的电压相角偏差与预期一致。利用本文所提攻击代价分析方法可以计算出单节点攻击和多节点攻击时需要篡改的量测数据个数分别为 24 个和 16 个。基于式(14)可求得单节点攻击向量(如表 5 所示)和多节点攻击向量(如表 6 所示)，其非零元素个数分别为 24 个和 16 个，与攻击代价理论分析计算值一致。此次攻击目标选择为零注入节点且攻击区域中零注入节点也较多，可明显看出单节点攻击和多节点攻击中攻击者需掌握的信息相同，但多节点攻击比单节点攻击所需篡改量测数更少。进一步分析发现，与对 IEEE-14 系统的攻击类似，攻击区域内的支路潮流量测值攻击后相比攻击前增长至少 1 倍，有可能会误导控制中心的判断，对电网安全稳定运行构成威胁。

表 5 IEEE-1354 系统中单节点攻击向量非零元素值

Table 5 Non-zero elements of multi-node attack vector of the IEEE-1354 system

$\Delta P_i/\Delta Q_i$	$\Delta p_{i\text{-}j}$	$\Delta q_{i\text{-}j}$
	$\Delta p_{10\text{-}34}$=−6.23	$\Delta q_{10\text{-}34}$=0.50
	$\Delta p_{34\text{-}10}$=6.21	$\Delta q_{34\text{-}10}$=−0.47
	$\Delta p_{10\text{-}893}$=6.43	$\Delta q_{10\text{-}893}$=−0.49
ΔP_{219}=−1.07	$\Delta p_{893\text{-}10}$=−6.45	$\Delta q_{893\text{-}10}$=0.53
ΔQ_{219}=0.10	$\Delta p_{34\text{-}219}$=1.05	$\Delta q_{34\text{-}219}$=−0.01
ΔP_{1349}=2.61	$\Delta p_{219\text{-}34}$=−0.89	$\Delta q_{219\text{-}34}$=−0.02
ΔQ_{1349}=0.26	$\Delta p_{893\text{-}1310}$=6.51	$\Delta q_{893\text{-}1310}$=−0.85
	$\Delta p_{1310\text{-}893}$=−6.52	$\Delta q_{1310\text{-}893}$=0.91
	$\Delta p_{1310\text{-}1349}$=7.28	$\Delta q_{1310\text{-}1349}$=−0.84
	$\Delta p_{1349\text{-}1310}$=−7.30	$\Delta q_{1349\text{-}1310}$=0.85

表 6 IEEE-1354 系统中多节点攻击向量非零元素值

Table 6 Non-zero elements of multi-node attack vector of the IEEE-1354 system

ΔP_i / ΔQ_i	$\Delta p_{i\text{-}j}$	$\Delta q_{i\text{-}j}$
	$\Delta p_{893\text{-}1310}$=2.28	$\Delta q_{893\text{-}1310}$=−0.25
ΔP_{219}=−1.07	$\Delta p_{1310\text{-}893}$=−2.28	$\Delta q_{1310\text{-}893}$=0.22
ΔQ_{219}=0.10	$\Delta p_{34\text{-}219}$=1.05	$\Delta q_{34\text{-}219}$=−0.01
ΔP_{1349}=−6.39	$\Delta p_{219\text{-}34}$=−0.89	$\Delta q_{219\text{-}34}$=−0.02
ΔQ_{1349}=0.58	$\Delta p_{1310\text{-}1349}$=0.54	$\Delta q_{1310\text{-}1349}$=−0.01
	$\Delta p_{1349\text{-}1310}$=−0.52	$\Delta q_{1349\text{-}1310}$=0.05

5 结论

本文根据电网实际运行特征选取攻击节点，以攻击节点为中心，构建单节点攻击区域和多节点攻击区域，针对这两种情形，基于交流系统状态估计模型，提出了一种掌握局部电网信息下的虚假数据注入攻击代价分析方法。分析发现限于攻击者所掌握资源，会尽可能压缩攻击成本，当进行多节点攻击时，如果选择具有相连支路的点作为攻击节点且使它们的电压相角偏差相同，可以大大缩减攻击成本，一定程度上还可提高攻击效率。最后以 IEEE-14 系统和 IEEE-1354 系统为例验证了本文所提攻击代价分析方法的有效性，可为电网安全稳定运行和网络安全防范提供参考。信息通信网的高速可靠运行与智能电网的发展推进和稳定运行息息相关，应逐步引起重视，下一步研究工作可着眼于虚假数据注入攻击强度对电网的影响分析及对应安全防范措施。

参考文献

[1] 李霞, 李勇, 曹一家, 等. 基于信息物理系统融合的光域互联电网阻尼控制策略[J]. 电力系统保护与控制, 2017, 45(21): 35-42.
LI Xia, LI Yong, CAO Yijia, et al. Wide-area damping control strategy of interconnected power grid based on cyber physical system[J]. Power System Protection and Control, 2017, 45(21): 35-42.

[2] 薛禹胜, 李满礼, 罗剑波, 等. 基于关联特性矩阵的电网信息物理系统耦合建模方法[J]. 电力系统自动化, 2018, 42(2): 11-19.
XUE Yusheng, LI Manli, LUO Jianbo, et al. Modeling method for coupling relations in cyber physical power systems based on correlation characteristic matrix[J]. Automation of Electric Power Systems, 2018, 42(2): 11-19.

[3] 倪明, 颜诘, 柏瑞, 等. 电力系统防恶意信息攻击的思考[J]. 电力系统自动化, 2016, 40(5): 1-4.
NI Ming, YAN Jie, BO Rui, et al. Power system cyber attack and its defense[J]. Automation of Electric Power Systems, 2016, 40(5): 1-4.

[4] 丁明, 李晓静, 张晶晶. 面向 SCADA 的网络攻击对电力系统可靠性的影响[J]. 电力系统保护与控制, 2018, 46(11): 37-45.
DING Ming, LI Xiaojing, ZHANG Jingjing. Effect of SCADA-oriented cyber attack on power system reliability[J]. Power System Protection and Control, 2018, 46(11): 37-45.

[5] 田继伟, 王布宏, 李夏. 智能电网状态维持拓扑攻击及其对经济运行的影响[J]. 电力系统保护与控制, 2018, 46(1): 51-56.
TIAN Jiwei, WANG Buhong, LI Xia. State-preserving topology attacks and its impact on economic operation of smart grid[J]. Power System Protection and Control, 2018, 46(1): 51-56.

[6] 赵俊华, 梁高琪, 文福拴, 等. 乌克兰事件的启示：防范针对电网的虚假数据注入攻击[J]. 电力系统自动化, 2016, 40(7): 149-151.
ZHAO Junhua, LIANG Gaoqi, WEN Fushuan, et al. Lessons learnt from the Ukrainian blackout: protecting power grids against false data injection attacks[J]. Automation of Electric Power Systems, 2016, 40(7): 149-151.

[7] LIU Y, NING P, REITER M K. False data injection attacks against state estimation in electric power grids[C] // Proceeding of the 16th ACM conference on Computer and Communications Security, November 9-13, 2009, Chicago, USA: 21-32.

[8] LIANG G, ZHAO J, LUO F, et al. A review of false data injection attacks against modern power systems[J]. IEEE Transactions on Smart Grid, 2017, 8(4): 1630-1638.

[9] VALENZUELA J, WANG J, BISSINGER N. Real-time intrusion detection in power system operations[J]. IEEE Transactions on Power Systems, 2013, 28(2): 1052-1062.

[10] YUAN Y, LI Z, KUI R. Quantitative analysis of load redistribution attacks in power system[J]. IEEE Transactions on Parallel and Distribution Systems, 2012, 23(9): 1731-1738.

[11] RAHMAN M A, MOHSENIAN-RAD H. False data injection attacks with incomplete information against smart power grids[C] // IEEE Global Communication Conference, December 3-7, 2012, Anaheim, USA: 3153-3158.

[12] ZHANG J, CHU Z, SANKAR L, et al. False data injection attacks on power system state estimation with limited information[C] // IEEE Power and Energy Society General Meeting, July 17-21, 2016, Boston, USA: 1-5.

[13] 代明明. 电力系统局部区域假数据注入攻击研究[D]. 成都: 西南交通大学, 2016.

[14] 李青芯, 孙宏斌, 盛同天, 等. 变电站状态估计中互感器虚假数据注入攻击分析[J]. 电力系统自动化, 2016, 40(17): 79-86.
LI Qingxin, SUN Hongbin, SHENG Tongtian, et al. Injection attack analysis of transformer false data in substation state estimation[J]. Automation of Electric Power Systems, 2016, 40(17): 79-86.

[15] YANG Q, YANG J, YU W, et al. On false data-injection attacks against power system state estimation: modeling and countermeasures[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(3): 717-729.

[16] DEKA D, BALDICK R, VISHWANATH S. Data attack on strategic buses in the power grid: design and protection[C] // IEEE PES General Meeting Conference & Exposition, July 27-31, 2014, National Harbor, USA: 1-5.

[17] 于尔铿. 电力系统状态估计[M]. 北京: 水利电力出版社, 1985.

[18] SANDBERG H, TEIXEIRA A, JOHANSSON K H. On security indices for state estimators in power networks[C] // Proceeding of the First Workshop on Secure Control Systems, April 14-16, 2010, Stockholm Sweden: 12-16.

[19] PASQUALETTI F, CARLI R, BULLO F. A distributed method for state estimation and false data detection in power networks[C] // IEEE International Conference on Smart Grid Communications, October 17-20, 2011, Brussels, Belgium: 469-474.

[20] RAHMAN M A, AI-SHAER E, KAVASSERI R G. A formal model for verifying the impact of stealthy attacks on optimal power flow in power grids[C] // IEEE International Conference on Cyber-Physical Systems, April 14-17, 2014, Berlin Germany: 175-186.

[21] HUG G, GIAMPAPA J A. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks[J]. IEEE Transactions on Smart Grid, 2012, 3(3): 1362-1370.

[22] RAHMAN M A, MOHSENIAN-RAD H. False data injection attacks against nonlinear state estimation in smart power grids[C] // IEEE Power & Energy Society General Meeting, July 21-25, 2013, Vancouver Canada: 1-5.

[23] LIANG J, KOSUT O, SANKAR L. Cyber attacks on AC state estimation: unobservability and physical consequences[C] // IEEE PES General Meeting Conference & Exposition, July 27-31, 2014, National Harbor, USA: 1-5.

收稿日期：2018-10-30；　修回日期：2019-02-03

作者简介：

赵丽莉(1988—)，女，通信作者，硕士，中级工程师，研究方向为电力信息物理系统分析；E-mail: zhaolili@sgepri.sgcc.com.cn

刘忠喜(1995—)，男，硕士研究生，研究方向为电网的状态估计与安全稳定。E-mail: liuzx0914@foxmail.com

(编辑　周金梅)